Requested Patent: WO03005185A1

Title:

METHOD OF SYSTEM PROTECTION FOR MICROSOFT WINDOWS 95/98/ME ;

Abstracted Patent: WO03005185 ;

Publication Date: 2003-01-16 ;

Inventor(s): CHAN KAM-FU (CN) ;

Applicant(s): CHAN KAM-FU (CN) ;

Application Number: WO2001IB01216 20010706 ;

Priority Number(s): WO2001IB01216 20010706 ;

IPC Classification: G06F9/00 ;

Equivalents: ;

ABSTRACT:

A method, resulting in the production of a customized running image of files, is provided for running off, through a customized booting process, Microsoft Windows 95/98/ME in protected WINDOWS mode under the protection of Input and Output System Driver(s) with built-in protection features against virus attacks and infections. The method and the booting process include the steps of producing a customized copy of configuration files used by Microsoft Windows 95/98/ME; copying these configuration files, system files provided by Microsoft Windows 95/98/ME during installation process and other device drivers and programmes to storage medium/media to be used in computer systems or devices capable of running Microsoft Windows 95/98/ME; and with the use of these files from the storage medium/ media, booting up in real DOS mode, preparing for and running off Microsoft Windows 95/98/ME in protected WINDOWS mode in these computer systems or devices.

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
16 January 2003 (16.01.2003)

PCT

(10) International Publication Number
WO 03/005185 A1

(51) International Patent Classification[7]: G06F 9/00

(21) International Application Number: PCT/IB01/01216

(22) International Filing Date: 6 July 2001 (06.07.2001)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant and
(72) Inventor: **CHAN, Kam-fu** [CN/CN]; Flat 2003, Block M, Allway Gardens, On Yat Street, Tsuen Wan, Hong Kong (CN).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

WO 03/005185 A1

(54) Title: METHOD OF SYSTEM PROTECTION FOR MICROSOFT WINDOWS 95/98/ME

(57) Abstract: A method, resulting in the production of a customized running image of files, is provided for running off, through a customized booting process, Microsoft Windows 95/98/ME in protected WINDOWS mode under the protection of Input and Output System Driver(s) with built-in protection features against virus attacks and infections. The method and the booting process include the steps of producing a customized copy of configuration files used by Microsoft Windows 95/98/ME; copying these configuration files, system files provided by Microsoft Windows 95/98/ME during installation process and other device drivers and programmes to storage medium/media to be used in computer systems or devices capable of running Microsoft Windows 95/98/ME; and with the use of these files from the storage medium/ media, booting up in real DOS mode, preparing for and running off Microsoft Windows 95/98/ME in protected WINDOWS mode in these computer systems or devices.

Description

Title of Invention:

METHOD OF SYSTEM PROTECTION FOR MICROSOFT WINDOWS 95/98/ME

Technical Field

This invention relates to system protection against virus attacks and infections whilst running Microsoft Windows 95/98/Millenium Edition (the operating system) in devices, including computer systems, capable of supporting the operating system. In particular, this invention relates to utilizing virtual container drive(s) and specially designed Input and Output System Driver(s) for protecting a customized running image of the operating system and other application(s) and data file(s) from virus attacks and infections whilst running in devices, including computer systems, capable of supporting the operating system.

Background Art

For any computer system or device capable of running it, Microsoft Windows 95/98/ME is designed to be installed onto and run on a non-volatile rewriteable storage medium with sufficient space and speed. Normally, the drive on which the operating system is installed cannot be write-protected if it is to be started into protected-mode.

A method for customizing the running image of the operating system so that it can be separated to be stored into System Drive and User Drive for

running into Windows protected-mode has been revealed in the invention contained in the International Application, PCT/IB00/01671, filed by CHAN Kam-fu (the same inventor of this application), with International Filing Date being 13 November 2000, received by International Bureau of the World Intellectual Property Organization. In that invention, the splitting of the running image of the operating system and other application(s) and data file(s) into System Drive and User Drive for running is for preserving modification(s), which are intended to be preserved, in User Drive. That is, modification(s) to be preserved are supposed to be written into User Drive for preservation. In this invention, however, the same customization for splitting the running image of the operating system and other application(s) and data file(s) into System Drive and User Drive is used for protecting the operating system and other application(s) and data file(s) that are supposed to be protected in System Drive against virus attacks and infections. This splitting customization allows the System Drive to be write-protected on and after starting into Windows protected-mode. Thus, all files so contained within the System Drive can be protected by either hardware or software or both.

The method of creating a CD capable of booting the full Microsoft Windows 98 at http://www.ct.heise.de/ct/english/99/11/206/ put forward by Tobias Remberg and Hajo Schulz is intended as a solution for creating a bootable CD for running Microsoft Windows 98. It involves the use of ramdisk for storing registry files and other temporary files. In this way, the CD cannot be removed, and as the running of the operating system relies on this non-rewriteable CD, which cannot be taken away while running, the running speed is slow. Besides, the method for splitting the operating system for running into two halves, one on ramdisk and the other on CD, revealed by them is not conceptualized into the notion of splitting the

running image to be stored separately in System Drive and User Drive for running purpose. And the method of the customization for split running revealed by them requires much more clarification and modification before it can be implemented for other purposes than creating a bootable CD for running Microsoft Windows 98. In their method, except those residing on ramdisk, most system files of the operating system are etched onto CD and thus protected by that piece of hardware without software intervention.

The present invention is an extension to the previously mentioned invention in the direction of protecting those parts of the operating system and other application(s) and data file(s) in System Drive under specially designed Input and Output drivers. Essentially, this invention includes a method of customization for splitting the running image of the operating system and other application(s) and data file(s) into System Drive and User Drive for running; whereby those parts intended to be protected against virus attacks and infections are protected in System Drive under the operation of specially designed Input and Output System Driver(s).

The specially designed Input and Output System Driver(s) here refer(s) to file system driver(s) and disk input/output driver(s) operating under real DOS mode and/or those under Windows protected-mode that are specially designed with built-in features for protecting drive(s) or areas under their supervision and management.

Up to now, operating systems are designed without much consideration given to protecting files from virus attacks and infections. The spread of different forms of virus attacks and infections in computers worldwide has caused increasing attention being given to developing protection methods for preventing damages caused by virus attacks and infections. Most of

these methods are software-based.

There are in general several kinds of software protection schemes. These include signature scanners, which scan executable files for recognizable signatures that could be used for virus identification and make correction or clean-up for those files so identified; heuristic scanners, which instead of looking for recognizable signatures look for recognizable instructions in executable files for virus identification and make correction or clean-up for those files so identified; integrity checkers, which make use of previously preserved checksum of executable files or other files and compare it with the new checksum of those files for virus detection and give alert to computer users; and activity monitors and blockers, which are resident programmes loaded into memory for constantly monitoring and blocking activities that are considered to be associated with virus attacks and infections.

All these software protection schemes are programmes that are added subsequently onto computer operating systems and external to file systems and disk input/output systems. Another scheme of protection that is offered by the ME version of the Microsoft Windows 95/98/ME series is called System File Protection. This System File Protection operates by detecting any changes to core Windows System Files and makes restoration afterwards by copying the previously unchanged or uninfected version of the files from a clean copy of the System Files. This System File Protection scheme though offered by the operating system still belongs to the category of activity monitors; instead of blocking operations of change, the operating system implements the process of restoring previously preserved unchanged version of system files. This scheme however does not protect other application files and data file(s) that are not part of the operating system.

All the above schemes of software protection have their strengths and weaknesses. This applies to this invention as well. However, this invention is original in the sense that it offers protection through adopting for use specially designed file system and/or disk input/output drivers with built-in features for system protection. This is made possible by the method of splitting of the system files of the operating system into protected System Drive, in the form of virtual container drive under the supervision and management of Input and Output System Driver(s), and updateable User Drive for running the operating system. From the moment of starting up the operating system, the specially designed Input and Output System Driver(s) offer protection to files, including operating system files, application files and data files, in designated drive(s) or areas under its / their supervision. Any write-operations directed to designated drive(s) or areas to be protected are translated into protective actions, including no-write operation, write-alert operation, write-redirection operation, write-translated-blocking operation, write-translated-killing operation, etc. as appropriate or as feasible. Besides such activity-translation actions, which prevents write-attacks, the implementation of translation algorithm(s) and non-native file system and / or disk format by the specially designed Input and Output System Driver(s) can also help contain the spread of virus infections for those viruses that are able to bypass the Input and Output System Driver(s) to do the write-attacks directly. The protection schemes offered by this invention could be classified as activity-translator and camouflaging.

The building of such protection features into the file system and disk input/output driver(s) has not been consciously implemented or adopted for use for the purpose of system protection against virus attacks and infections so far. This is due to the fact that Microsoft Windows 95/98/ME, or other

operating systems, is intended to be installed onto re-writeable storage medium which is not intended to be write-protected. Implementing a native read-only file system and / or disk input/output driver for protecting a particular drive or directory of the re-writeable storage medium does not appear to be a natural way for protecting system files. This is because of the simple fact that those system files which are intended to be protected have to be written or installed through the file system and disk input/output driver(s) onto the System Drive hosted on a re-writeable storage medium first before it can be run. The native file system and disk input/output driver(s) tend(s) therefore to be both read-enabled and write-enabled. For Microsoft Windows 95/98/ME, even if native file system and disk input/output driver(s) with both write-enabled and write-disabled capabilities are designed (so far there have been no write-disabled native FAT16 and FAT32 input/output drivers designed for use under real DOS mode and under protected WINDOWS mode), there has so far been no systematic revelation of how the operating system can be started up from a rewriteable storage medium under the supervision of write-disabled or read-only file system and/or disk input/output driver(s). This is revealed in this invention.

The problem at present is that most of the available virtual container drive drivers implement only one aspect or another of the system protection features in their input/output system. Also, they may not be available both under real DOS mode and protected WINDOWS mode, nor may they be in compatible form under both of these modes.

This is because the existing virtual container drive drivers are all designed for purpose other than what is explicated in this invention. Encryption / Decryption software is designed for providing data security so that data are

prevented from being known by unauthorized users. Compression / Decompression software is designed for saving disk space. NTFS, HPFS, Ext2 and other file system and / or disk format drivers are designed for reading under real DOS mode or under protected WINDOWS mode files stored in NTFS, HPFS, Ext2 or other file system and / or disk format. These files are previously written onto them under the operation of other different operating systems such as Windows NT / 2000, OS2, Linux, etc.

There are plenty of such prior art available free or as commercial products in the market for selection. Very often the read-only forms of these virtual container drive drivers are usually designed as demos or giveaways for attracting potential customers to buy their read-and-write counterparts. They are not designed with the purpose of system protection against virus attacks and infections in mind.

The key factor of not building protection features into the Input and output System Driver(s) is oblivion to user needs and the necessity for enabling the write-operation routines for the initial installation procedure for the very operation systems in question. As mentioned earlier, for Microsoft Windows 95/98/ME in particular, there has not been any systematic revelation about how the system files can be separated into two parts to be stored in System Drive for protection from change and in User Drive for preserving change. This invention therefore explicates how this can be done and how the operating system can be started off into protected WINDOWS mode successfully with the system files divided into System Drive and User Drive under the supervision of specially designed Input and Output System Driver(s) for system protection against virus attacks and infections.

For instances, at present two READONLY Input and Output System

Drivers are found to be compatible under real DOS mode and protected WINDOWS mode for use in protecting the System Drive on and after starting up the operating system. One is iHPFS, released by Marcus Better under GNU General Public License, for reading files stored in HPFS format. The other, WinShield, is developed by Windrive International Limited, incorporated in Hong Kong. WinShield is a specially designed Input and Output System Driver implementing a specially designed disk format for the purpose of system protection, especially developed for implementing the features of this invention. At present, it offers two modes, read-write mode and read-only mode for mounting drives intended for different purposes. For instances, during development stage, read-write mode is available for both System Drive and User Drive. Whereas during production run, System Drive is placed into read-only mode and User Drive in read-write mode. Other enhancement system protection features as described below in the section of Disclosure of Invention can be built into the driver as well.

For Microsoft Windows ME, another problem of protecting it under real DOS mode Input and Output System Driver(s) is due to the disabling of real DOS mode during the hard disk boot-up process in this version of Microsoft Windows. This suppression of real DOS mode makes loading real DOS mode drivers through CONFIG.SYS and/or real DOS mode programmes through AUTOEXEC.BAT or through real DOS command prompt impossible when Microsoft Windows ME boots up from a hard disk. To be able to load real DOS mode drivers or programmes, one has to boot up from the Emergency Boot Disk (prepared by Microsoft Windows ME) placed in the booting floppy drive. This creates great inconvenience. This problem, however, can be solved by writing a software which enables real DOS mode hard disk booting by making patches to IO.SYS,

COMMAND.COM in the root directory of the hard disk boot-up drive and REGENV32.EXE in the \WINDOWS\SYSTEM directory. One such software, Real DOS-Mode Patch for Windows ME v1.3, has been released on the Internet. According to the document accompanying the software, Real DOS-Mode Patch for Windows ME v1.3 was released on 15 August 2000 by a group called MANiFEST DESTiNY with a website, which appears, at the time of writing, to be engaging in other business instead of software development.

Disclosure of Invention

This invention reveals a method of running Microsoft Windows 95/98/ME in protected System Drive with the advantage of automatically preventing modifications to files intended to be protected in System Drive during running the operating system. Other files whose modifications are considered normal or not amenable to protection from modification because of the need for system running, such as configuration files, registry files and swap file, are to be stored on User Drive.

This invention includes a method for customizing the configuration and preparing a running image of the operating system so that it can be run off in protected WINDOWS mode in protected System Drive together with other application file(s) and data file(s) intended to be protected from modification stored therewith. User configuration and other files whose modifications are considered normal or not amenable to protection from modification are stored on a rewriteable storage medium that can be recognized as a User Drive. A System Drive is defined as a virtual container drive under the supervision and management of Input and Output System Driver(s), including file system and / or disk input/output driver(s),

which has / have built-in features offering protection to files, including files of the operating system and /or application files and / or data files, stored therein against virus attacks and infections. Such Input and Output System Driver(s) can be real DOS mode driver(s) and / or protected WINDOWS mode driver(s).

With the possibility of starting up the operating system from a virtual container drive or an area under the supervision of write-disabled or read-only Input and Output System Driver(s), including file system and / or disk input/output driver(s), better protection features can be built into this / these driver(s) as enhanced protection schemes.

Virtual container drive is defined here as a computer file or file container which, when opened or mounted by Input and Output System Driver(s) capable of using it, appears to be a drive with a compatible file system format capable of holding other files that are accessible under real DOS mode and protected WINDOWS mode. Such virtual container drive may be in the form of any native drives that are normally supervised by the native Input and Output System Driver(s) of the operating system; in the case of Microsoft Windows 95/98/ME, they are FAT16 and FAT32 drives by default. If the native FAT16 and/or FAT32 drive(s) are used as file containers for system protection against virus attacks and infections, the specially designed Input and Output System Driver(s) should be able to replace the native Input and Output System Driver(s) of the operating system in supervising these default drive(s).

The basic feature of the specially designed Input and Output System Driver(s) for system protection against virus attacks and infections is to disable any actions involving write-operations in at least the lowest disk

input/output level; such disabling of any write-operations can also be implemented in the file system level as well.

Enhancement of system protection against virus attacks and infections can be achieved by re-directing any write-operations on the protected System Drive to the location or drive specially designated for storing such unintended modifications for logging and detection purpose. Other possibilities include giving alerts to users if any unexpected write-operations are detected and starting up any other enhancement functions, such as killing or stopping the suspected target application that initiates those unexpected write-operations.

Translation algorithm(s) can also be built into the read-operation and write-operation routines as another form of protection. This may be useful for preventing any virus attacks, which are capable of bypassing the read and write operations of the supervising Input and Output System Driver(s) by directly writing onto the underlying file system and disk formats, from being able to spread their impact onto other files under protection. If the supervising Input and Output System Drivers are built in with translation algorithm(s) in read-operation routines and write-operation routines, any virus write-operations which bypass these Input and Output System Drivers may not write correctly because these virus write-operations could not correctly write data without knowing the translation algorithm(s) used. So when these data are read back, they become scrambled by the translation algorithm(s) built into the read-operation routines and are therefore rendered meaningless and not executable for the purpose of spreading further virus attacks and infections.

The write-operation routines are supposed to be disabled or re-defined as

described above when in production mode, i.e. when the system is actually running for production purpose. These write-operation routines are only enabled for writing data when in development mode, i.e. when the system is not running for production. The development mode is a stage of preparing the system for actual running for production; such as installing, copying and preparing the operating system itself as well as other application files and data files into the System Drive.

The translation algorithm(s) adopted are usually decryption or decompression algorithm for the read-operations and encryption or compression algorithm for the write-operations.

Better protection feature can also be implemented by re-defining the format of the underlying logical and physical structure of the file system and disk format as implemented by the Input and Output System Driver(s). For instance, the supervising Input and Output System Driver(s) can use HPFS, NTFS, Ext2 or any other specially designed formats. These formats are distinguished from the native underlying logical and physical structure of file system and disk format as implemented by the native file system and disk input/output driver(s) inherently built into the operating systems, i.e. the FAT16 and FAT32 formats. The use of a different file system and / or disk format offers better protection. This is because any virus attacks which bypass the supervising Input and Output System Driver(s) for their write-operations may not know correctly what exactly is the underlying logical and physical file system and disk format for recording data.

The use of translation algorithm(s) and different logical and physical file system and disk format therefore make it very difficult for virus attacks, which use the technique of writing directly to the underlying disk by

bypassing the supervising Input and Output System Driver(s), to write correctly. If they fail to write correctly, what they write cannot be correctly read back. This may render the disk damaged and unusable at most but can prevent any possibility of further virus spread or virus infection.

So specially designed Input and Output System Driver(s) offer(s) built-in system protection features against virus attacks and infections in the following manners. If virus attacks use Input and Output System Driver(s) for any write-operations, the write-operation routines of the Input and Output System Driver(s) translate the normal write-operations into system protection routines as described above. These write-translated operations include no-write operations, re-directing write-operations to designated area for logging and detecting, alerting function, starting up killing or stopping routines against targeted application, etc.

Should virus attacks be able to bypass Input and Output System Driver(s) and write directly onto the storage medium on which the System Drive is hosted, the adoption of translation algorithm(s) and non-native file system and disk format by the specially designed Input and Output System Driver(s) may also prevent virus infections from further spreading from the damaged storage medium on which the System Drive is hosted.

The advantage of building system protection features into Input and Output System Driver(s) over other activity monitoring, blocking and killing programmes or device drivers added externally onto Input and Output System Driver(s) is due to the fact that certain viruses can be of the same class of these programmes or device drivers. These viruses may also attempt to kill, stop or bypass the monitoring abilities of these programmes or device drivers.

Should viruses try to take over the role of Input and Output System Driver(s) in managing direct read-operations and write-operations, it is very difficult for them to detect or predict correctly what translation algorithm(s) and file system and disk format are used. So their damages are limited to the storage medium on which the System Drive is hosted so that the danger of widespread virus infection can be prevented.

The method described in this invention therefore leads to the creation of a product, i.e. a customized image of files consisting of customized configuration files, system files of the operating system, specially designed Input and Output System Drivers and other relevant programmes; the use of which makes possible the phenomenon of running off Microsoft Windows 95/98/ME in protected WINDOWS mode with system files, other application file(s) and data file(s) protected in System Drive(s) under the supervision of specially designed Input and Output System Driver(s) in computer systems or devices capable of running the operating system. To support specially designed real DOS mode Input and Output System Driver(s) for the ME version of Microsoft Windows 95/98/ME, one has to boot up from the Emergency Boot Disk (prepared by Microsoft Windows ME) placed in the booting floppy drive or to use a software which enables real DOS mode hard disk booting by making patches to IO.SYS, COMMAND.COM in the root directory of the hard disk boot-up drive and REGENV32.EXE in the \WINDOWS\SYSTEM directory.

The method includes the steps of customizing the configuration of the running image of Microsoft Windows 95/98/ME; transferring or copying the properly configured running image (including system image and user configuration), specially designed Input and Output System Driver(s) and other relevant programmes, application files and data files as the case may

be into System Drive(s) and User Drive(s) as appropriate on storage medium/media; booting off the running image in real DOS mode; loading the specially designed DOS mode Input and Output System Driver(s) if any; running SUBST.EXE command if necessary; and finally issuing the command, WIN, under real DOS mode to start the operating system in protected WINDOWS mode and loading specially designed protected WINDOWS mode Input and Output System Driver(s) if any.

These steps are detailed as follows:

1. Customizing the configuration of the running image of Microsoft Windows 95/98/ME

Before customizing the existing configuration files, all existing configuration files, or better, all files have to be backed up first so that the existing operation system and its configuration is preserved. A new copy of these configuration files for use with a new copy of the running image of the operating system is then to be produced.

To configure a running image of Microsoft Windows 95/98/ME suitable for protecting system files, other application file(s) and data file(s) in System Drive against virus attacks and infections under the supervision of specially designed Input and Output System Driver(s) involves the following sub-steps:

(a) Customizing configuration files read by the operating system under real DOS mode

Microsoft Windows 95/98/ME can be made to boot up in two phases,

the first phase is booting to real DOS mode. The second phase is booting to protected WINDOWS mode by issuing the WIN command. In the first phase, it reads in IO.SYS, MSDOS.SYS, COMMAND.COM, CONFIG.SYS, and AUTOEXEC.BAT, if available and applicable, for user-configurable system information, commands and programmes to be executed. In the process, it prepares for loading into protected WINDOWS mode. It starts its protected-mode operation after the WIN command is issued.

(1) Customizing MSDOS.SYS

After issuing the WIN command, the operating system tries to load Microsoft Windows 95/98/ME into protected WINDOWS mode. Before this is successful, the operating system checks the system information about where the Microsoft Windows 95/98/ME WINDOWS system files are located. This information is stored in RAM on booting and specified in MSDOS.SYS. Modifying MSDOS.SYS after booting does not change the system information stored in RAM. So for the operating system to locate these system files and run the protected-mode Microsoft Windows 95/98/ME successfully, MSDOS.SYS should contain proper settings before the operating system boots up under real DOS mode. The relevant settings for the location of the WINDOWS system files of Microsoft Windows 95/98/ME are specified under the section:

[Paths]
WinDir=
WinBootDir=
HostWinBootDrv=

WinDir specifies where the WINDOWS system files are located. If the virtual container drive, representing the System Drive, which is used for holding the system image files, is mounted as V: drive, and the WINDOWS system files, excluding WIN.COM (for this invention, WIN.COM has to be placed under a directory as specified by WinBootDir= setting, but including WIN.COM in the directory specified by WinDir= setting has no adverse effect in operation), i.e. the files of the Windows directory, are put into a directory named '\WINDOWS', then WinDir should be set as WinDir=V:\WINDOWS.

WinBootDir specifies where the command, WIN.COM, is stored. In this invention, this setting should be different from the setting of WinDir. WinDir should be set as the directory on the virtual container drive, representing the System Drive, where all WINDOWS system files except WIN.COM are placed (however, including WIN.COM in the WinDir= directory has no adverse effect in operation). WinBootDir= should be set to a directory on a rewriteable storage medium recognized as a drive, representing the User Drive, under real DOS mode before the operating system is started into protected WINDOWS mode. In this directory, besides WIN.COM, user configuration files used by the operating system when it is started into and running in protected WINDOWS mode are also placed. These user configuration files include at least all Registry files and all INI files; Policy files and User Profile files may be included as well. Besides these files, the file folders, Desktop and Start Menu, and all the files and sub-file folders within these two file folders of the installed Windows directory should also be included. If the drive containing these files is recognized as U: drive, and all these files and file folders are placed into a directory called \WINDOWS, the WinBootDir=

should be set as WinBootDir=U:\WINDOWS.

HostWinBootDrv specifies which drive that boots up the operating system. This setting can be set as the actual boot-up drive.

The setting:

[Options]
DisableLog=

controls whether Bootlog.txt is created during the booting process. It assumes the value 1 or 0. This setting should be included and set so as to disable the creation of Bootlog.txt on booting up if the booting storage medium is a read-only medium.

The setting:

[Options]
SystemReg=

controls whether the booting process scans the system registry or not. It assumes the value 1 or 0. In certain cases, the configuration of running Microsoft Windows 95/98/ME off for system protection against virus attacks and infections may have changed the default location of the system registry, enabling this setting to 1 will lead to booting error. To ensure that the operating system boots up properly in all cases, this setting should be set to 0 to disable scanning system registry;

(2) Customizing CONFIG.SYS and AUTOEXEC.BAT

It is recommended that the LastDrive setting in CONFIG.SYS under the root directory of the boot-up drive be set to Z so as to allow using all 26 drive letters.

As said before, on booting up to real DOS mode, the operating system prepares for running in protected WINDOWS mode. It reads in MSDOS.SYS to find out where the system files are. By default, the WinDir and WinBootDir are assumed to be C:\WINDOWS if they are not set otherwise in MSDOS.SYS. Using such information, the operating system loads HIMEM.SYS and IFSHLP.SYS in the case of Microsoft Windows 95/98 or IFSHLP.SYS only in the case of Microsoft Windows ME. The driver(s) should be loaded in memory before WIN.COM is started so that the operating system can be run in protected WINDOWS mode.

If the driver(s), HIMEM.SYS and IFSHLP.SYS in the case of Microsoft Windows 95/98 or IFSHLP.SYS in the case of Microsoft Windows ME, is/are not found in the directory specified by WinDir= in MSDOS.SYS, the driver(s) cannot be loaded and the operating system cannot be started into protected WINDOWS mode. If the driver(s) is/are put elsewhere, the loading of which can however be made possible by specifying their location(s) in CONFIG.SYS with the use of the DEVICE= or DEVICEHIGH= statements. Another way of loading device driver can be done by writing a device-loading programme to be executed under real DOS, either to be specified in AUTOEXEC.BAT or to be executed under DOS command prompt. Whatever is the way, the driver(s) should be loaded before WIN.COM

is issued for protected-mode Microsoft Windows 95/98/ME to run.

Other device drivers such as specially designed real DOS mode Input and Output System Driver(s) for supervising the System Drive (a virtual container drive) and/or User Drive and/or CDROM driver, if necessary as the case may be, have to be loaded as appropriate, before WIN command is issued. This is done by specifying in CONFIG.SYS, or in AUTOEXEC.BAT or loaded under DOS command prompt as the case may be.

Because of the setup location of the System Drive and the need for better protecting the boot-up drive, depending on configuration, sometimes SUBST.EXE command(s) has/have to be issued before issuing the WIN command. For instance, if the System Drive is set up as drive X:, and the boot-up device or drive is recognized as C:, then the command [drive:][path]SUBST.EXE C: X:\ can be used. Implementing [drive:][path] SUBST.EXE [host drive:] [mounted drive:]\ will also improve re-usability of any running session; where [host drive:] is the drive hosting the virtual container drive and [mounted drive:] is the mounted virtual container drive. SUBST.EXE command(s) can be put in AUTOEXEC.BAT or issued at DOS command prompt before the WIN command.

Set Path= or Path= / Path statement(s) can be included in CONFIG.SYS or AUTOEXEC.BAT to facilitate locating programmes or utilities to be executed under real DOS command prompt for loading drivers and mounting virtual container drive.

Two additional settings in AUTOEXEC.BAT are relevant to Microsoft

Windows ME. They are SET windir= and SET winbootdir= . These two settings should be made identical to the settings of windir= and winbootdir= as specified in MSDOS.SYS.

Because the System Drive is supposed to be write-protected basically, so temporary files created by the operating system and other applications should be designated onto other re-writeable drive or location. So SET TEMP= and SET TMP= in AUTOEXEC.BAT should be set to re-writeable location(s) other than in the System Drive.

(b) Customizing configuration files read by the operating system after issuing the WIN command

The configuration files read by the operating system during and after the process of loading into protected WINDOWS mode are the Registry files, Policy files, User Profile files, and INI files. These files contained various entries of system and user configuration information. To ensure that the operating system loads successfully into protected-mode operation, the entries containing the location, i.e. the precise drive and directory information, of the running image of the operating system should be altered accordingly. For instance, if the running image of the operating system (except WIN.COM, the entries pointing to the location of which within configuration files have to be set to that specified by WinBootDir=) is to be found in V:\WINDOWS and at the moment the entries in these configuration files point to C:\WINDOWS, then all these entries have to be changed to pointing V:\WINDOWS. This applies to other directory or location information for other application programmes correspondingly in their respective

locations.

However, for this invention, as Registry files and INI files (Policy files and User Profile files are optional) are now placed under the WinBootDir= directory, any entries within these configuration files referring to the location of these configuration files themselves have to be customized to point to the WinBootDir= directory. In this case, for example, the WinBootDir= should be different from the V:\WINDOWS; it may be set to pointing to a directory on the rewriteable storage medium drive, such as WinBootDir=U:\WINDOWS. So any entries within configuration files referring to the location of the configuration files themselves have to be set likewise to U:\WINDOWS, instead of V:\WINDOWS.

Also for this invention, another particular entry within the Registry files has to be set to that specified by the setting of WinBootDir=. This is the following key within the Registry:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\SystemRoot

This setting directs the operating system to store relevant user configuration information whilst running. The operating system also reads in information contained in file folders of Desktop and Start Menu of the WinBootDir= directory (also specified in the above key within the Registry) for starting up the user environment in relation to the Desktop configuration and Start Menu information.

The Registry files, Policy files and User Profile files cannot be easily

altered under real DOS mode. For convenience, these files have to be altered after the protected WINDOWS mode is running. Because these files contain many entries about directory information, a programme has to be developed for such alteration. Suppose if the operating system now starts from C:\WINDOWS, it will crash if all entries in the Registry files pointing to C:\WINDOWS are altered to V:\WINDOWS if the process is not done properly and restored afterwards. Therefore, these configuration files have to be backed up first and used later for recovery in case of system crash during the alteration process. The programme capable of doing such alteration has to, firstly change the relevant entries so that they point to their valid new location(s), secondly copy the new configuration files to another location for use later, and finally change back the relevant entries in the configuration files so that they point to their unaltered location(s). Otherwise, the operating system will crash.

INI files have also to be changed likewise.

Settings for specifying the location of Swap or Paging file contained under the [386Enh] section in the SYSTEM.INI should not be set to point to any location or target in the System Drive, which is supposed to be write-protected basically. There are two such settings; namely PagingDrive= and PagingFile=.

The location(s) of programmes specified in Shortcut files should also be changed to their new location(s) so that they can be validly referred to and run successfully.

After the above steps of customization, the existing operating system

is preserved and a new copy of MSDOS.SYS, CONFIG.SYS, AUTOEXEC.BAT, Registry files, Policy files, User Profiles, INI files and Shortcut files is produced.

Another way of obtaining suitable configuration files of a running image is to partition and format a hard disk with sufficient number of drives, and then install the operating system onto the appropriate drive, the drive letter of which will later be taken up by the virtual container drive on which the running image is to run. For instance, if drive V: is to be used as the System Drive containing the system files of the operating system for running off the operating system, the hard disk should first be partitioned and formatted up to drive V:, and a new installation of the operating system is set up on this drive V:. The running image will be suitable for running from the System Drive. Other configuration files of MSDOS.SYS, CONFIG.SYS, and AUTOEXEC.BAT should however be customized as appropriate; these files together with IO.SYS, COMMAND.COM, HIMEM.SYS and IFSHLP.SYS in case of Microsoft Windows 95/98 or IFSHLPS.SYS in case of Microsoft Windows ME, and Input and Output System Driver(s) are to be placed on the boot-up drive in appropriate locations. WIN.COM, Registry files, Policy files, User Profiles, INI files and file folders of Desktop and Start Menu and their sub-folders and files are to be placed under a directory as specified by WinBootDir= on a User Drive created on a rewriteable storage medium that can be recognized and used under real DOS mode before the operating system starts into protected WINDOWS mode.

WinDir= should be set to the \WINDOWS directory (assuming where the Windows system files except WIN.COM are placed) of the System

Drive for indicating the location of all Windows system files except WIN.COM and WinBootDir= set to a directory on user configuration directory in User Drive created on rewriteable storage medium for indicating the location of WIN.COM and user configuration information. The SystemRoot key within the Registry mentioned above should likewise be set to that specified by WinBootDir=. Other settings within configuration files pointing to Windows system files should be set to that specified by WinDir=, except WIN.COM and the configuration files, whose entries are set to WinBootDir=.

After backing up the running image and the associated customized configuration files, the hard disk should be re-partitioned to have less number of drives so that a free drive letter V: can be taken up by the System Drive under the supervision and management of its Input and Output System Driver(s) if the System Drive is not in native FAT16 or FAT32 format. If the System Drive is to be in native FAT16 or FAT32 format, then the Input and Output System Driver(s) associated with the System Drive should be able to replace the native Input and Output System Driver(s) in providing system protection features upon booting up and starting to run. A User Drive has to be created on a rewriteable storage medium for storing WIN.COM and user configuration files as described above (including Registry files, INI files as well as Desktop and Start Menu file folders and their sub-folders and files; and optionally Policy files, User Profile files) so that they can be available for reading and writing by the operating system when it is started up into protected WINDOWS mode.

The whole customized running image thus contains the following files to be stored in User Drive and System Drive and boot-up drive if

boot-up drive is different from User Drive or System Drive. Configuration files to be read under real DOS booting, together with IO.SYS, COMMAND.COM are to be placed on the boot-up drive. HIMEM.SYS and IFSHLP.SYS in the case of Microsoft Windows 95/98 and IFSHLP.SYS only in the case of Microsoft Windows ME, as well as real DOS mode Input and Output System Driver(s) for System Drive and/or User Drive are to be placed in location that is accessible for loading upon real DOS booting up. Configuration files and WIN.COM to be used on starting the operating system into and running it in protected WINDOWS mode are to be placed in a User Drive created on a rewriteable storage medium recognized under real DOS mode. Device drivers such as storage device driver(s), virtual container drive driver(s), i.e. the Input and Output System Driver(s) for virtual container drive(s), programmes or utilities for loading and utilizing these drivers, and all other Windows system files (WIN.COM may be excluded) supplied by the operating system during the installation process as selected by the user are to be placed in the virtual container drive, representing the System Drive.

2. Transferring the customized running image onto storage medium/media

This stage is the Development Stage for preparing the running image. The Input and Output System Driver(s) supervising and managing the System Drive should be loaded and write-enabled for the purpose of copying. User Drive can be in the native FAT16 or FAT32 format. If not, the User Drive Input and Output System Driver(s), which is/are supposed to be write-enabled no matter in Development stage or Production stage, should be loaded up. This is so for boot-up drive if

it is different from System Drive and User Drive.

After loading all the relevant write-enabled Input and Output System Driver(s), to copy this customized running image of the operating system, one can start up the operating system in protected WINDOWS mode and make use of EXPLORER.EXE to copy all the files of the customized running image to brand-new drives, one for the System Drive, one for the User Drive, another for the boot-up drive if it is different from the System Drive and the User Drive. If EXPLORER.EXE is used, the WIN386.SWP system swap file cannot be copied. This file therefore has to be deselected for copying purpose. It will be created afresh on next running.

Configuration files to be read under real DOS booting, together with IO.SYS, COMMAND.COM are to be copied onto the boot-up drive, which should be made bootable under real DOS mode.

HIMEM.SYS and IFSHLP.SYS in the case of Microsoft Windows 95/98 and IFSHLP.SYS only in the case of Microsoft Windows ME are to be copied to location that is accessible for loading upon real DOS booting up. This is also applicable to any real DOS mode Input and Output System Driver(s).

WIN.COM, Registry files, INI files as well as Desktop and Start Menu file folders and their sub-folders and files, and optionally Policy files and User Profile files, have to be copied to a directory specified by the WinBootDir= setting in a User Drive, whether in the form of another virtual container drive or ordinary hard disk drive in native FAT16 or FAT32 format. This User Drive should be accessible upon

the real DOS mode booting so that user configuration information can be read and WIN.COM be executed for booting the operating system in protected WINDOWS mode.

Device drivers such as storage device driver(s), virtual container drive driver(s), i.e. the Input and Output System Driver(s) for virtual container drive(s), programmes or utilities for loading and utilizing these drivers, and all other Windows system files (WIN.COM may be excluded) supplied by the operating system during the installation process as selected by the user are to be copied to the virtual container drive, representing the System Drive, in their respective locations accessible before and upon booting into protected WINDOWS mode.

At present, except for employing WinShield, there have been no such Input and Output System Drivers that can be switched between read-write mode for development and read-only mode for production run and that are compatible under both real DOS mode and protected WINDOWS mode for the purpose of this invention.

Without suitable Input and Output System Drivers which are compatible under both real DOS mode and protected WINDOWS mode for reading from and writing onto the virtual container drive representing the System Drive during this Development Stage, Microsoft Windows 95/98/ME cannot be used for the purpose of copying the customized running image onto at least the System Drive, which is supposed to be write-protected on production run.

To illustrate how convoluted this copying process can be when there is no compatible driver like WinShield is, iHPFS is used as an

example. iHPFS, as mentioned earlier in Background Art section, is the only other available Input and Output System Driver that is found to be compatible both under real DOS mode and protected WINDOWS mode and can be used for the purpose of this invention. iHPFS is however a read-only driver under real DOS mode and protected WINDOWS mode. To copy the corresponding image files onto the System Drive to be supervised by iHPFS, one has to use either OS2 or Windows NT 3.51 or NT 4.0.

In this case, the System Drive to be supervised by iHPFS under Microsoft Windows 95/98/ME is in HPFS format. A HPFS drive has therefore to be created by OS2 or created by some other disk partitioning software such as Partition Magic. After creating this HPFS drive, one has to fire up OS2 in a computer within which the customized running image so produced under Microsoft Windows 95/98/ME should be found on a FAT16 drive recognizable by OS2. Then one can use OS2 for copying the corresponding customized running image files onto the System Drive in HPFS format.

Windows NT 3.51 and 4.0 can also be used for copying by installing Pinball.sys onto the system. This allows them to read and write onto HPFS drive. However, the HPFS drive, representing the System Drive, cannot be created under Windows NT 3.51 or 4.0. So OS2 or some other utilities such as Partition Magic must first be used for creating the HPFS drive.

This means that one has to have either OS2 or Windows NT 3.51 or 4.0 installed on the same computer as Microsoft Windows 95/98/ME is on. Otherwise, one has to remove hard disk or similar storage

medium from one machine to another and then vice versa.

3. Booting off the customized running image in real DOS mode

To boot off the customized running image in real DOS mode and to access it later, the booting device has to gain access to the storage medium/media on which the boot-up drive, the System Drive and the User Drive are stored; the boot-up drive may also be the same as System Drive or User Drive as the case may be.

The image of the following files, namely, IO.SYS, MSDOS.SYS, CONFIG.SYS, COMMAND.COM, and AUTOEXEC.BAT, should be stored in the root directory of the boot-up drive or the contents of such files can be read for the purpose of booting. MSDOS.SYS, CONFIG.SYS, and AUTOEXEC.BAT have to be configured as described above.

HIMEM.SYS and IFSHLP.SYS in the case of Microsoft Windows 95/98 or IFSHLP.SYS in the case of Microsoft Windows ME, storage device driver and Input and Output System Drive(s) for the virtual container drive(s), representing the System Drive and / or the User Drive are also required to be available for loading before issuing the WIN command.

4. Starting into protected WINDOWS mode

After booting off into real DOS mode, the real DOS mode Input and Output System Driver(s) for virtual container drive(s), representing the System Drive and/or the User Drive if any, should be loaded for

gaining access to the virtual container drive(s). At this stage of production running, the real DOS mode Input and Output System Driver for the System Drive should be in read-only mode at least. Other built-in system protection features of the driver may be activated if available and found appropriate.

For some configuration, the SUBST.EXE command(s) has/have to be issued before issuing the WIN command. For instance, if the boot-up drive is different from the System Drive or the User Drive, for its better protection, SUBST.EXE command may be issued to make it hide behind the System Drive or the User Drive. Also if the customization process supposes the System Drive to be at V:, and if the System Drive at boot-up appears as J:, then SUBST.EXE command has also to be issued so that V: is made referring to J:.

The User Drive containing user configuration files and WIN.COM should be accessible upon real DOS mode booting. After all the above drives are in place, issuing WIN command will execute the WIN.COM stored in the User Drive. This starts the process of booting into protected WINDOWS mode and in the process, user configuration information stored in the directory specified by the setting of WinBootDir= is read in and used. In this way, the Windows system image stored in the System Drive will be loaded and the operating system starts running in protected WINDOWS mode. After starting into protected WINDOWS mode, specially designed protected WINDOWS mode Input and Output System Driver(s) for System Drive and/or User Drive if any should also be loaded for enhanced protection and better operation.

Best Mode for Carrying out the Invention

Because of the complexity of the process of customizing the configuration of the running image of the operating system and the convoluted procedure for copying the corresponding running image files onto the virtual container drive representing the System Drive, the best mode for carrying out the invention involves the use in a computer of Input and Output System Driver(s), which are compatible both under real DOS mode and protected WINDOWS mode, for the virtual container drive representing the System Drive both in the development stage and in the production run.

The Input and Output System Driver(s) should be able to be switched from read-write mode in the development stage for preparing the customized running image consisting of the operating system, other application files and data files, to read-only mode during the production run. Other enhanced system protection features built into the Input and Output System Driver(s) for the System Drive are activated as the case may be during production run.

Industrial Applicability

Microsoft Windows 95/98/ME is at present the most popular operating system in the world. Its widespread use also makes it the most obvious target for virus attacks and infections. This has exacted tremendous resources from the computing community using the operating system for containing virus attacks and infections.

There is no panacea to this headache.

This invention has its weaknesses as well. However, with the use of this invention, by putting the system files of the operating system (and other application files and data files if so desired for protection) into a System Drive supervised and managed by its Input and Output System Driver(s) with built-in features of system protection against virus attacks and infections, this headache may be lessened.

As mentioned earlier, this method of system protection against virus attacks and infections has advantage over existing anti-virus protection methods in that the system protection features are built into Input and Output System Driver(s). With the implementation of suitable combination of protection features, including write-disablement, write-redirection, write-alert, and other write-translated actions, virus attacks could be minimized and an uninfected copy of system files capable of running every time can be preserved. With additional implementation of built-in translation algorithm(s) and non-native file system and disk format, Input and Output System Driver(s) are able to contain the infection attacks of those viruses that are able to bypass the Input and Output System Driver(s).

The prior art for the implementation of this invention includes the operating system of Microsoft Windows 95/98/ME; the hardware of any devices, including computer systems, capable of running Microsoft Windows 95/98/ME; the specifications of booting these devices, including computer systems, under real DOS mode; in the case of Microsoft Windows ME, the software for enabling access to real DOS mode (by patching IO.SYS, COMMAND.COM and REGENV32.EXE) during the booting process if the IO.SYS and COMMAND.COM of Emergency Boot Disk prepared by Microsoft Windows ME are not used; various kinds of storage device drivers, Input and Output System Driver(s) with built-in protection features

for virtual container drive(s) representing System Drive and/or User Drive; programmes or utilities for loading and utilizing these device drivers; and programmes or utilities, including other operation systems, such as OS2 and Windows NT 3.51 and 4.0, for copying files into virtual container drive(s) and their creation for use with Microsoft Windows 95/98/ME.

In combination with the use of the technical features contained in the prior art stated above, this invention makes possible the phenomenon of running off Microsoft Windows 95/98/ME in protected WINDOWS mode from a protected System Drive under the supervision and management of its Input and Output System Driver(s) with built-in protection features against virus attacks and infections and, in this relation, is characterized by the following claims:

Claims

1. A method, capable of being implemented in computer-executable programme(s) and/or computer-executable instruction(s), comprising steps, in any form of combination as the case may be, of preparing and producing a copy of customized running image of files copied or transferred to storage medium / media to be used for running off Microsoft Windows 95/98/ME in protected WINDOWS mode in computer systems or devices capable of running the operating system, whereby this customized running image of files are to be stored in System Drive, User Drive and boot-up drive (if boot-up drive is not the same as System Drive or User Drive) for booting and whereby upon booting the System Drive is protected against virus attacks and infections under the supervision and management of its Input and Output System Driver(s), including file system and/or disk input/output driver(s) operating under real DOS Mode and/or under protected WINDOWS mode, with built-in protection features against virus attacks and infections, including features, implemented individually or in any combination as the case may be, of write-disablement; write-redirection; write-alerts; write-translated actions, such as blocking and/or killing viruses and their viral actions; built-in translation algorithm(s) for read and/or write operations; non-native file system and/or disk format(s);
2. A customized copy of MSDOS.SYS as contained in the said copy of customized running image of files as specified in Claim 1;
3. The said copy of MSDOS.SYS of Claim 2 containing customized entry of WinDir= pointing to the location of system files of Microsoft Windows 95/98/ME in System Drive;
4. The said copy of MSDOS.SYS of Claim 2 containing customized

entry of WinBootDir= pointing to the booting directory, the location of WIN.COM, in User Drive on rewriteable storage medium for running protected-mode Microsoft Windows 95/98/ME;

5. The said copy of MSDOS.SYS of Claim 2 containing customized entry of HostWinBootDrv= pointing to the boot-up drive;

6. The said copy of MSDOS.SYS of Claim 2 containing customized entry of DisableLog= being set to 1 for disabling the creation of BOOTLOG.TXT on booting up if so used;

7. The said copy of MSDOS.SYS of Claim 2 containing customized entry of SystemReg= being set to 0 for disabling the scanning of system registry if so used;

8. A customized copy of CONFIG.SYS as contained in the said copy of customized running image of files as specified in Claim 1;

9. The said copy of CONFIG.SYS of Claim 8 containing customized entry of LastDrive= to specify the last available drive letter, thus the number of available drives for use, so as to provide for the inclusion of Input and Output System Driver(s) for supervising and managing the virtual container drive(s) representing System Drive and/or User Drive, and/or storage device(s) as the case may be; for maximizing the number of available drives, setting it to Z;

10. The said copy of CONFIG.SYS of Claim 8 containing customized entry of SET PATH= to facilitate locating programmes for utilizing devices, including Input and Output System Driver(s) for supervising and managing the virtual container drive(s) representing System Drive and/or User Drive if so used, and/or storage device(s); and/or to facilitate locating other programmes for execution, in particular SUBST.EXE and WIN.COM;

11. The said copy of CONFIG.SYS of Claim 8 containing customized entry of Device= or DeviceHigh= to accommodate the inclusion and

loading of HIMEM.SYS in case of Microsoft Windows 95/98;

12. The said copy of CONFIG.SYS of Claim 8 containing customized entry of Device= or DeviceHigh= to accommodate the inclusion and loading of IFSHLP.SYS;

13. The said copy of CONFIG.SYS of Claim 8 containing customized entry or entries of Device= and/or DeviceHigh= to accommodate the inclusion and loading of real DOS mode Input and Output System Driver(s) for the virtual container drive representing System Drive;

14. The said copy of CONFIG.SYS of Claim 8 containing customized entry or entries of Device= and/or DeviceHigh= to accommodate the inclusion and loading of real DOS mode Input and Output System Driver(s) for the virtual container drive representing User Drive if so used;

15. The said copy of CONFIG.SYS of Claim 8 containing customized entry or entries of Device= and/or DeviceHigh= to accommodate the inclusion and loading of storage device driver(s);

16. A customized copy of AUTOEXEC.BAT as contained in the said copy of customized running image of files as specified in Claim 1;

17. The said copy of AUTOEXEC.BAT of Claim 16 containing customized entry of SET windir= pointing to the directory of the WinDir= setting in MSDOS.SYS;

18. The said copy of AUTOEXEC.BAT of Claim 16 containing customized entry of SET winbootdir= pointing to the directory of WinBootDir= setting in MSDOS.SYS;

19. The said copy of AUTOEXEC.BAT of Claim 16 containing customized entry of PATH or PATH= to facilitate locating programmes for utilizing devices, including Input and Output System Driver(s) for virtual container drive(s) representing System Drive and/or User Drive if so used, and/or storage device(s); and/or to

facilitate locating other programmes for execution, in particular SUBST.EXE and WIN.COM.

20. The said copy of AUTOEXEC.BAT of Claim 16 containing customized entry or entries of SET TEMP= and/or SET TMP=, where the entry or entries are set to a location other than in System Drive.

21. The said copy of AUTOEXEC.BAT of Claim 16 containing customized entry for executing programme for loading HIMEM.SYS in case of Microsoft Windows 95/98;

22. The said copy of AUTOEXEC.BAT of Claim 16 containing customized entry for executing programme for loading IFSHLP.SYS;

23. The said copy of AUTOEXEC.BAT of Claim 16 containing customized entry or entries for executing programme(s) for loading and utilizing storage device driver(s);

24. The said copy of AUTOEXEC.BAT of Claim 16 containing customized entry or entries for executing programme(s) for loading and utilizing real DOS mode Input and Output System Driver(s) for the virtual container drive representing System Drive;

25. The said copy of AUTOEXEC.BAT of Claim 16 containing customized entry or entries for executing programme(s) for loading and utilizing real DOS mode Input and Output System Driver(s) for the virtual container drive representing User Drive if so used;

26. The said copy of AUTOEXEC.BAT of Claim 16 containing customized entry or entries for executing SUBST.EXE;

27. The said copy of AUTOEXEC.BAT of Claim 16 containing customized entry for executing WIN.COM;

28. A customized copy of Registry files as contained in the said copy of customized running image of files as specified in Claim 1 and in particular wherein the key of

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\
CurrentVersion\SystemRoot
is set to the directory as specified by WinBootDir= setting in MSDOS.SYS;

29. A customized copy of Policy files as contained in the said copy of customized running image of files as specified in Claim 1;

30. A customized copy of User Profile files as contained in the said copy of customized running image of files as specified in Claim 1;

31. A customized copy of INI files as contained in the said copy of customized running image of files as specified in Claim 1;

32. A customized copy of Shortcut files as contained in the said copy of customized running image of files as specified in Claim 1;

33. The said steps of Claim 1 comprising the step to the effect of producing a copy of customized configuration files, in any form of combination as the case may be, to be read under real DOS mode on booting, such files including:

(a) Claim 2 with customized entries as specified in Claims 3 to 7 in any form of combination as the case may be;

(b) Claim 8 with customized entries as specified in Claims 9 to 15, in any form of combination as the case may be, where Claim 11 is applicable to Microsoft Windows 95/98 only; and

(c) Claim 16 with customized entries as specified in Claims 17 to 27, in any form of combination as the case may be, where Claims 17 and 18 are applicable to Microsoft Windows ME only and Claim 21 is applicable to Microsoft Windows 95/98 only;

34. The said steps of Claim 1 comprising the step to the effect of producing a copy of customized configuration files, including Claims 28 to 32 in any form of combination as the case may be, to be read by Microsoft Windows 95/98/ME when starting into protected

WINDOWS mode; where any entries in these configuration files relating to the locations of files used by Microsoft Windows 95/98/ME are customized to pointing to their valid locations; in particular entries relating to locations of files in System Drive are pointed to their valid locations in System Drive, and entries for files in User Drive are pointed to their valid locations in User Drive as the case may be; in particular where the PagingDrive= and/or PagingFile= entry or entries under the [386Enh] section of SYSTEM.INI should be set to a target or location other than that in the System Drive.

35. The said steps of Claim 1 comprising the step to the effect of copying or transferring:

(a) files selected as the case may be from files provided by Microsoft for setting up a running image of Microsoft Windows 95/98/ME or from files of a running image of Microsoft Windows 95/98/ME (in the case of Microsoft Windows ME, including IO.SYS, COMMAND.COM and REGENV32.EXE, which have been enabled to allow access to real DOS mode in the booting process); and/or

(b) the customized copy of configuration files as specified in Claims 2, 8 and 16 in any form of combination as the case may be; and/or

(c) the customized copy of configuration files as specified in Claims 28 to 32 in any form of combination as the case may be; and/or

(d) the file folders, Desktop and Start Menu, and all the files and sub-file folders within these two file folders of the installed Windows directory; and/or

(e) Input and Output System Driver(s) for System Drive and/or User Drive if so used, and storage device driver(s) in any form of combination as the case may be; and

(f) other application files and/or data files if so used as the case may be;

to valid locations of virtual container drive(s) (virtual container drive being defined as a computer file or file container that is accessible, mountable and recognizable as a compatible drive wherein the files so contained are accessible for use by Microsoft Windows 95/98/ME), including and acting as, as the case may be, System Drive and User Drive that have been created on or are subsequently copied or transferred to storage medium, which can be recognized as logical drive(s) and can be used in the booting process by the booting device of a computer system or device capable of running Microsoft Windows 95/98/ME so that System Drive (in the form of virtual container drive) upon booting up is protected against virus attacks and infections under the supervision and management of its Input and Output System Driver(s) with built-in protection features; and User Drive, stored on rewriteable storage medium, is accessible under real DOS mode booting for use in starting Microsoft Windows 95/98/ME into protected WINDOWS mode;

36. The said steps of Claim 1 comprising the step to effect of copying or transferring

(a) IO.SYS and COMMAND.COM (which have been enabled to allow access to real DOS mode in the booting process in the case of Microsoft Windows ME), as well as HIMEM.SYS and IFSHLP.SYS in the case of Microsoft Windows 95/98 or IFSHLP.SYS in the case of Microsoft Windows ME;

(b) the customized copy of configuration files as specified in Claims 2, 8 and 16 in any form of combination as the case may be; and

(c) Input and Output System Driver(s) and storage device driver(s) in any form of combination as the case may be,

to storage medium / media wherein they are placed in valid location(s) of logical drive(s) that can be recognized and used in the booting

process by the booting device of a computer system or device capable of running Microsoft Windows 95/98/ME;

37. The step to the effect of reading in IO.SYS and COMMAND.COM, and if available and as the case may be MSDOS.SYS, CONFIG.SYS and AUTOEXEC.BAT, as contained in the customized running image of files so produced as specified in Claim 1;

38. The step to the effect of loading HIMEM.SYS and IFSHLP.SYS in the case of Microsoft Windows 95/98 or IFSHLP.SYS in the case of Microsoft Windows ME as contained in the customized running image of files so produced as specified in Claim 1;

39. The step to the effect of loading and preparing real DOS Mode Input and Output System Driver(s) for virtual container drive(s) representing System Drive and / or User Drive if so used and, if available and as the case may be, storage device driver(s) as contained in the customized running image of files so produced as specified in Claim 1 for use;

40. The step to the effect of issuing the command(s) SUBST.EXE to substitute one drive for another, if necessary, so that through substitution the relevant entries of configuration files (as contained in the customized running image of files so produced as specified in Claim 1) relating to the locations of files used by Microsoft Windows 95/98/ME are pointing to their valid locations, in particular entries relating to the locations of files in System Drive are so pointing to their valid locations in System Drive and entries relating to the locations of files in User Drive on rewriteable storage medium are so pointing to their valid locations in User Drive on rewriteable storage medium;

41. The step to the effect of issuing WIN.COM for running off

Microsoft Windows 95/98/ME into protected WINDOWS mode; and during the process, the customized running image of files so produced as specified in Claim 1 is used, resulting in the loading of protected WINDOWS mode Input and Output System Driver(s) for supervising and managing System Drive and/or User Drive if so used as the case may be;

42. A method of booting off the customized running image of files copied or transferred to storage medium / media so produced as specified in Claim 1 under real DOS mode into protected WINDOWS mode; wherein the booting process, through executing computer-executable programme(s) or computer-executable instruction(s), including but not limited to using the customized configuration files as specified in Claims 2, 8 and 16 in any form of combination as the case may be and the customized configuration files as specified in Claims 28 to 32 in any form of combination as the case may be, executes the steps as specified in Claims 37 to 41 as the case may be to the effect that Microsoft Windows 95/98/ME runs into protected WINDOWS mode with System Drive protected by its Input and Output System Driver(s) with built-in protection features against virus attacks and infections;

43. The customized running image of files so produced as the case may be and copied or transferred to storage medium / media as specified in Claim 1; and

44. The use of the customized running image of files so produced as the case may be and copied or transferred to storage medium / media as specified in Claim 1 in computer system(s) or device(s) capable of running Microsoft Windows 95/98/ME.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/IB01/01216

A. CLASSIFICATION OF SUBJECT MATTER

IPC[7] G06F 9/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC[7] G06F 9/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

NONE

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

WPI EPODOC PATENTPIC PAJ RS 清华非专利文献库：msdos sys programm+ driv+ protected mode configuaration 保护模式 启动 系统文件 驱动 配置

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriPate, of the relevant passages	Relevant to claim No.
A	US5794245A 11/Aug/1998 IPC6 G06F 17/30 whole document	1-44
A	US5581788A 3/Dec/1996 IPC6 G06F 15/02 whole document	1-44
A	US5278973A 11/Jan/1994 IPC5 G06F 9/22 whole document	1-44
A	CN1170160A 14/Jan/1998 IPC6 G06F 12/00 whole document	1-44
A	Windos95 和 DOS 两系统中 MSDOS.SYS 的作用与设置 《内蒙古科技与经济》1999 年第 4 期	1-44
A	利用 Msdos.sys 配置 Windows 95 的启动 《长春邮电学院学报》1999 年 第 17 卷 第 3 期	1-44

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim (S) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
26.Dec.2001(26.12.01)	17 JAN 2002 (17.01.02)
Name and mailing address of the ISA/CN 6 Xitucheng Rd., Jimen Bridge, Haidian District, 100088 Beijing, China Facsimile No. 86-10-62019451	Authorized officer 3307 Telephone No. 86-10-62093195

Form PCT/ISA /210 (second sheet) (July 1998)